

(e) Third-country transfers. The release or disclosure of foreign government information to any third-country entity must have the prior consent of the originating government if required by a treaty, agreement, bilateral exchange, or other obligation.

### Subpart E—Self-Inspections

#### § 2001.60 General [5.4].

(a) *Purpose.* This subpart sets standards for establishing and maintaining an ongoing agency self-inspection program, which shall include the periodic review and assessment of the agency's classified product. "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under the Order.

(b) *Applicability.* These standards are binding on all executive branch agencies that create or handle classified information. Pursuant to Executive Order 12829, the National Industrial Security Program Operating Manual (NISPOM) prescribes the security requirements, restrictions and safeguards applicable to industry, including the conduct of contractor self-inspections. The standards established in the NISPOM should be consistent with the standards prescribed in Executive Order 12958, as amended and this part.

(c) *Responsibility.* The senior agency official is responsible for the agency's self-inspection program. The senior agency official shall designate agency personnel to assist in carrying out this responsibility.

(d) *Approach.* The official(s) responsible for the program shall determine the means and methods for the conduct of self-inspections. These may include:

- (1) A review of relevant security directives, guides and instructions;
- (2) Interviews with producers and users of classified information;
- (3) A review of access and control records and procedures; and
- (4) A review of a sample of classified documents generated by agency activities.

(e) *Frequency.* The official(s) responsible for the program shall set the frequency of self-inspections on the basis of program needs and the degree of

classification activity. Activities that generate significant amounts of classified information should conduct at least one document review per year.

(f) *Reporting.* The format for documenting findings shall be set by the official(s) responsible for the program.

#### § 2001.61 Coverage [5.4(d)(4)].

(a) *General.* These standards are not all-inclusive. Each agency may expand upon the coverage according to program and policy needs. Each self-inspection of an agency activity need not include all the elements covered in this section. Agencies without original classification authority need not include in their self-inspections those elements of coverage pertaining to original classification.

(b) *Elements of coverage.* (1) Original classification. (i) Evaluate original classification authority's general understanding of the process of original classification, including the:

(A) Applicable standards for classification;

(B) Levels of classification and the damage criteria associated with each; and

(C) Required classification markings.

(ii) Determine if delegations of original classification authority conform with the requirements of the Order, including whether:

(A) Delegations are limited to the minimum required to administer the program;

(B) Designated original classification authorities have a demonstrable and continuing need to exercise this authority;

(C) Delegations are in writing and identify the official by name or position title; and

(D) New requests for delegation of classification authority are justified.

(iii) Assess original classification authority's familiarity with the duration of classification requirements, including:

(A) Assigning a specific date or event for declassification that is less than 10 years when possible;

(B) Establishing ordinarily a 10 year duration of classification when an earlier date or event cannot be determined; and

(C) Limiting extensions of classification for specific information not to exceed 25 years for permanently valuable records or providing a 25 year exemption.

(iv) Conduct a review of a sample of classified information generated by the inspected activity to determine the propriety of classification and the application of proper and full markings.

(v) Evaluate classifiers' actions to comply with the standards specified in § 2001.15 and § 2001.32 of this part, relating to classification and declassification guides, respectively.

(vi) Verify observance with the prohibitions on classification and limitations on reclassification.

(vii) Assess whether the agency's classification challenges program meets the requirements of the Order and this part.

(2) Derivative classification. Assess the general familiarity of individuals who classify derivatively with the:

(i) Conditions for derivative classification;

(ii) Requirement to consult with the originator of the information when questions concerning classification arise;

(iii) Proper use of classification guides; and

(iv) Proper and complete application of classification markings to derivatively classified documents.

(3) Declassification.

(i) Verify whether the agency has established, to the extent practical, a system of records management to facilitate public release of declassified documents.

(ii) Evaluate the status of the agency declassification program, including the requirement to:

(A) Comply with the automatic declassification provisions regarding historically valuable records over 25 years old;

(B) Declassify, when possible, historically valuable records prior to accession into the National Archives;

(C) Provide the Archivist with adequate and current declassification guides;

(D) Ascertain that the agency's mandatory review program conforms to established requirements; and

(E) Determine whether responsible agency officials are cooperating with the ISOO Director to coordinate the linkage and effective utilization of existing agency databases of records that have been declassified and publicly released.

(4) Safeguarding.

(i) Monitor agency adherence to established safeguarding standards.

(ii) 5.4(c) of the Order—Verify whether the agency has established to the extent practical a records system designed and maintained to optimize the safeguarding of classified information.

(iii) Assess compliance with controls for access to classified information.

(iv) Evaluate the effectiveness of the agency's program in detecting and processing security violations and preventing recurrences.

(v) Assess compliance with the procedures for identifying, reporting and processing unauthorized disclosures of classified information.

(vi) Evaluate the effectiveness of procedures to ensure that:

(A) The originating agency exercises control over the classified information it generates;

(B) Holders of classified information do not disclose information originated by another agency without that agency's authorization; and

(C) Departing or transferred officials return all classified information in their possession to authorized agency personnel.

(5) Security education and training. Evaluate the effectiveness of the agency's security education and training program in familiarizing appropriate personnel with classification procedures; and determine whether the program meets the standards specified in subpart F of this part.

(6) Management and oversight.

(i) Determine whether original classifiers have received prescribed training.

(ii) Verify whether the agency's special access programs:

(A) Adhere to specified criteria in the creation of these programs;

(B) Are kept to a minimum;

(C) Provide for the conduct of internal oversight; and

(D) Include an annual review of each program to determine whether it continues to meet the requirements of the Order.

(iii) Assess whether:

(A) Senior management demonstrates commitment to the success of the program, including providing the necessary resources for effective implementation;

(B) Producers and users of classified information receive guidance with respect to security responsibilities and requirements;

(C) Controls to prevent unauthorized access to classified information are effective;

(D) Contingency plans are in place for safeguarding classified information used in or near hostile areas;

(E) The performance contract or other system used to rate civilian or military personnel includes the management of classified information as a critical element or item to be evaluated in the rating of: Original classifiers; security managers; classification management officers; and security specialists; and other employees whose duties significantly involve the creation or handling of classified information; and

(F) A method is in place for collecting information on the costs associated with the implementation of the Order.

### Subpart F—Security Education and Training

#### § 2001.70 General [5.4].

(a) *Purpose.* This subpart sets standards for agency security education and training programs. Implementation of these standards should:

(1) Ensure that all executive branch employees who create, process or handle classified information have a satisfactory knowledge and understanding about classification, safeguarding, and declassification policies and procedures;

(2) Increase uniformity in the conduct of agency security education and training programs; and

(3) Reduce improper classification, safeguarding and declassification practices.

(b) *Applicability.* These standards are binding on all executive branch departments and agencies that create or handle classified information. Pursuant to Executive Order 12829, the NISPOM prescribes the security requirements, restrictions, and safeguards applicable to industry, including the conduct of contractor security education and training. The standards established in the NISPOM should be consistent with the standards prescribed in Executive Order 12958, as amended and of this part.

(c) *Responsibility.* The senior agency official is responsible for the agency's security education and training program. The senior agency official shall designate agency personnel to assist in carrying out this responsibility.

(d) *Approach.* Security education and training should be tailored to meet the specific needs of the agency's security program, and the specific roles employees are expected to play in that program. The agency official(s) responsible for the program shall determine the means and methods for providing security education and training. Training methods may include briefings, interactive videos, dissemination of instructional materials, and other media and methods. Agencies shall maintain records about the programs it has offered and employee participation in them.

(e) *Frequency.* The frequency of agency security education and training will vary in accordance with the needs of the agency's security classification program. Each agency shall provide some form of refresher security education and training at least annually.

#### § 2001.71 Coverage [5.4(d)(3)].

(a) *General.* Each department or agency shall establish and maintain a formal security education and training program which provides for initial and refresher training, and termination briefings. This subpart establishes security education and training standards for original classification authorities, declassification authorities, security managers, classification management officers, security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information. These